Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2005/017305

International filing date: 20 September 2005 (20.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-308554
Filing date: 22 October 2004 (22.10.2004)

Date of receipt at the International Bureau: 28 October 2005 (28.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年１０月２２日
出願番号 Application Number:	特願２００４－３０８５５４
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－３０８５５４
出願人 Applicant(s):	日本電信電話株式会社

２００５年１０月１２日

特許庁長官
Commissioner,
Japan Patent Office

中嶋　誠

【書類名】　特許願
【整理番号】　NTTH166078
【提出日】　平成16年10月22日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/46
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　瀬林　克啓
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　倉上　弘
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　副島　裕司
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　エリック　チェン
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　冨士　仁
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100089118
　【弁理士】
　【氏名又は名称】　酒井　宏明
【選任した代理人】
　【識別番号】　100114306
　【弁理士】
　【氏名又は名称】　中辻　史郎
【手数料の表示】
　【予納台帳番号】　036711
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0310351

【書類名】特許請求の範囲
【請求項１】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置であって、
前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、
前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、
を備えたことを特徴とする中継装置。
【請求項２】
前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、
前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、
前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項１に記載の中継装置。
【請求項３】
攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手段を備え、
当該シグネチャ生成手段は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項２に記載の中継装置。
【請求項４】
前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を他の隣接中継装置に送信するとともに、当該シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、当該シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報および容疑シグネチャを前記シグネチャ記憶手段に対応付けて登録し、
前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されている場合には、当該生成識別情報に対応付けて登録されている中継元情報が前記受信したシグネチャの中継元情報と同一であるか否かをさらに判定し、
前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に既に登録されているが、前記中継元情報が同一であると判定された場合には、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に上書き登録するとともに、当該シグネチャを前記シグネチャ記憶手段に登録されている中継先情報が示す他の隣接中継装置に送信することを特徴とする請求項３に記載の中継装置。
【請求項５】
前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記中継元情報が同一でないと判定された場合には、前記シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送し、さらに、当該既登録通知を他の隣接中継装置から受信した場合には、前記シグネチャ記憶手段に記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除することを特徴とする請求項

４に記載の中継装置。
【請求項６】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、
前記中継装置は、
前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、
前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、
を備えたことを特徴とするネットワーク攻撃防御システム。
【請求項７】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継方法であって、
前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定工程と、
前記識別情報判定工程によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信工程と、
を含んだことを特徴とする中継方法。
【請求項８】
前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、
前記シグネチャ登録判定工程は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、
前記シグネチャ通信工程は、前記シグネチャ登録判定工程によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項７に記載の中継方法。
【請求項９】
攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成工程を含み、
当該シグネチャ生成工程は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項８に記載の中継方法。
【請求項１０】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、
前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手順と、
前記識別情報判定手順によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手順と、

をコンピュータに実行させることを特徴とする中継プログラム。
【請求項１１】
前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、
前記シグネチャ登録判定手順は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、
前記シグネチャ通信手順は、前記シグネチャ登録判定手順によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項１０に記載の中継プログラム。
【請求項１２】
攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手順をコンピュータに実行させ、
当該シグネチャ生成手順は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項１１に記載の中継プログラム。

【書類名】明細書
【発明の名称】中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システム
【技術分野】
【０００１】
この発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャリストに登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムに関する。
【背景技術】
【０００２】
従来より、防御対象であるコンピュータが接続されたネットワーク上に複数の中継装置を有し、ＤｏＳ（Denial of Service）攻撃またはＤＤｏＳ（Distributed Denial of Service）攻撃を受けるコンピュータを防御するネットワーク攻撃防御システムが知られている。例えば、特許文献１（特開２００３－２８３５５４号公報）や特許文献２（特開２００３－２８３５７２号公報）に開示されたネットワーク攻撃防御システムでは、中継装置において、予め決められた攻撃容疑パケットの検出条件に通信トラヒックが合致するか否かをチェックする。そして、合致したトラヒックを検出した場合に、中継装置は、検出された攻撃容疑パケットの伝送帯域制限値を表すシグネチャを生成して隣接中継装置（隣接関係をもつ中継装置）へ送信するとともに、以後、シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行う。
【０００３】
一方、シグネチャを受信した中継装置（隣接中継装置）では、通過するパケットの伝送帯域をシグネチャによって表される伝送帯域制限値に制限するとともに、さらに上流の隣接中継装置に対してシグネチャを送信する。つまり、シグネチャを受信した各中継装置がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置が同様のシグネチャに基づいてパケットを処理し、これによって、各中継装置を通過するパケットの伝送帯域をシグネチャが示す伝送帯域制限値に制限する。なお、上流または下流の中継装置とは、隣接中継装置であり、かつ攻撃容疑パケットが流入する方向に対する中継装置である。
【０００４】
さらに、一定時間経過後、攻撃を検出した中継装置は、各隣接中継装置から攻撃容疑パケットの平均入力伝送帯域値を受信し、各隣接中継装置における平均入力伝送帯域の比率により伝送帯域制限調整値を算出し、算出した伝送帯域制限調整値を隣接中継装置に送信する。そして、かかる伝送帯域制限調整値を受信した中継装置は、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整しながら、さらに上流の隣接中継装置に伝送帯域制限調整値を送信する。つまり、伝送帯域制限調整値を受信した各中継装置が伝送帯域制限調整値の送信を繰り返すことで、ネットワーク上の全ての中継装置が同様の伝送帯域制限調整値を受信し、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整する。
【０００５】
【特許文献１】特開２００３－２８３５５４号公報
【特許文献２】特開２００３－２８３５７２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
ところで、上記した従来の技術は、隣接中継装置にシグネチャを送信するので、ネットワーク攻撃防御システムにおける互いの中継装置の隣接関係によっては、異なる隣接中継装置から同一のシグネチャを受信する中継装置が存在することがある。そして、このような中継装置では、重複したシグネチャに基づいた処理を行う結果、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができないという問題がある。以下に、図１２および図１３を用いて、この問題を具体的に説明する。図１２および図１３は、従

来技術に係るネットワーク攻撃防御システムを説明するための図である。

【０００７】

図１２に示すように、中継装置９－１は、２つの通信端末３０がネットワーク上のサーバ２０に対するＤＤｏＳ攻撃を行っていることを検出すると（同図の（１）参照）、シグネチャを隣接中継装置となる中継装置９－２および中継装置９－３に送信する（同図の（２）参照）。そして、隣接中継装置となる中継装置９－１からシグネチャを受信した中継装置９－２は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャを隣接中継装置となる中継装置９－３に送信する。同様に、隣接中継装置となる中継装置９－１からシグネチャを受信した中継装置９－３は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャを隣接中継装置となる中継装置９－２に送信する（同図の（３）参照）。なお、図１２に示す例では、隣接中継装置からシグネチャを受信した中継装置９は、自己に送信した隣接中継装置にはシグネチャを送信しない。

【０００８】

このようなシグネチャの送信が行われると、図１２に示す例では、中継装置９－３は、隣接中継装置となる中継装置９－１および中継装置９－２から同一のシグネチャを受信することになる。また、これと同様に、中継装置９－２も、隣接中継装置となる中継装置９－１および中継装置９－３から同一のシグネチャを受信することになる。その結果、中継装置９－２および中継装置９－３では、重複したシグネチャに基づいたパケット制御処理を行うことになり、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができない。

【０００９】

また、図１３に示すように、中継装置９－１は、２つの通信端末３０がネットワーク上のサーバ２０に対するＤＤｏＳ攻撃を行っていることを検出すると（同図の（１）参照）、シグネチャを隣接中継装置となる中継装置９－２および中継装置９－３に送信する（同図の（２）参照）。そして、隣接中継装置となる中継装置９－１からシグネチャを受信した中継装置９－２および中継装置９－３は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャをそれぞれの隣接中継装置となる中継装置９－４に送信する（同図の（３）参照）。

【００１０】

このようなシグネチャの送信が行われると、図１３に示す例では、中継装置９－４は、隣接中継装置となる中継装置９－２および中継装置９－３から同一のシグネチャを受信することになる。その結果、中継装置９－２および中継装置９－３では、重複したシグネチャに基づいたパケット制御処理を行うことになり、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができない。

【００１１】

そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことが可能な中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

【課題を解決するための手段】

【００１２】

上述した課題を解決し、目的を達成するため、請求項１に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置であって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、を備えたことを特徴とする。

【００１３】
また、請求項２に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。
【００１４】
また、請求項３に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手段を備え、当該シグネチャ生成手段は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。
【００１５】
また、請求項４に係る発明は、上記の発明において、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を他の隣接中継装置に送信するとともに、当該シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、当該シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報および容疑シグネチャを前記シグネチャ記憶手段に対応付けて登録し、前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されている場合には、当該生成識別情報に対応付けて登録されている中継元情報が前記受信したシグネチャの中継元情報と同一であるか否かをさらに判定し、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に既に登録されているが、前記中継元情報が同一であると判定された場合には、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に上書き登録するとともに、当該シグネチャを前記シグネチャ記憶手段に登録されている中継先情報が示す他の隣接中継装置に送信することを特徴とする。
【００１６】
また、請求項５に係る発明は、上記の発明において、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記中継元情報が同一でないと判定された場合には、前記シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送し、さらに、当該既登録通知を他の隣接中継装置から受信した場合には、前記シグネチャ記憶手段に記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除することを特徴とする。
【００１７】
また、請求項６に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、前記中継装置は、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、を備えたことを特徴とする。
【００１８】

また、請求項７に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継方法であって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定工程と、前記識別情報判定工程によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信工程と、を含んだことを特徴とする。

【００１９】

また、請求項８に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定工程は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信工程は、前記シグネチャ登録判定工程によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

【００２０】

また、請求項９に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成工程を含み、当該シグネチャ生成工程は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。

【００２１】

また、請求項１０に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手順と、前記識別情報判定手順によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手順と、をコンピュータに実行させることを特徴とする。

【００２２】

また、請求項１１に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定手順は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信手順は、前記シグネチャ登録判定手順によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

【００２３】

また、請求項１２に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手順をコンピュータに実行させ、当該シグネチャ生成手順は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に

対応付けて登録することを特徴とする。
【発明の効果】
【００２４】
請求項１、６、７または１０の発明によれば、隣接中継装置から受信したシグネチャが既に登録されているか否かを判定して、未だ登録されていないシグネチャのみをシグネチャ記憶手段（シグネチャリスト）に登録するとともに隣接中継装置に送信するので、シグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。
【００２５】
また、請求項２、８または１１の発明によれば、シグネチャの生成を一意に識別するための生成識別情報（生成元である中継装置を一意に識別するための識別子および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子からなる生成識別情報）を各シグネチャに対応付けて管理するので、シグネチャの具体的な内容にまで踏み込むことなく、生成識別情報のみからシグネチャが既に登録されているか否かを判定することが可能になる。また、シグネチャの内容が同一であっても生成識別情報（生成元）が異なっていれば、未だ登録されていないシグネチャであるとしてシグネチャリストに登録するとともに隣接中継装置に送信するので、生成元となる各中継装置の性能違い（例えば、攻撃検出や防御解除に係るアルゴリズムの違いなど）が尊重され、安全性の高いパケット制御を行うことが可能になる。
【００２６】
また、請求項３、９または１２の発明によれば、攻撃容疑パケットを検出すると、シグネチャおよび生成識別情報を生成し、これらシグネチャおよび生成識別情報を隣接中継装置に送信するとともに、中継先である隣接中継装置を特定するための中継先情報、生成識別情報およびシグネチャをシグネチャリストに対応付けて登録するので、シグネチャに対して確実に生成識別情報を付与することが可能になる。また、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリストに登録された中継先情報、生成識別情報およびシグネチャを参照することで、同一の生成識別情報が付与されたシグネチャを同一の中継先に対して確実に再送信することが可能になる。
【００２７】
また、請求項４の発明によれば、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに未だ登録されていない場合には、これを他の隣接中継装置に送信するとともに、シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、生成識別情報およびシグネチャをシグネチャリストに対応付けて登録する。そして、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに既に登録されている場合には、中継元情報が同一であるか否かをさらに判定し、これが同一である場合には、シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている中継先情報が示す他の隣接中継装置にシグネチャを送信するので、送信ミスや内容更新等に起因してシグネチャが再送信されてきた場合でも、このシグネチャを留めることなく、中継先に対して確実に再送信することが可能になる。その一方、中継元情報が同一でない場合には、シグネチャの再送信でもないと判定される結果、シグネチャの重複登録や重複送信を確実に回避することが可能になる。
【００２８】
また、請求項５の発明によれば、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに既に登録されており、かつ、中継元情報も同一でない場合には、シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。さらに、当該既登録通知を他の隣接中継装置から受信した場合には、シグネチャリストに記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除する。したがって、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリストから削除された中継先に対してはシグネチ

ャが送信されないことになり、シグネチャの再送信に際してもシグネチャの重複登録や重複送信を確実に回避することが可能になる。

【発明を実施するための最良の形態】

【００２９】

以下に添付図面を参照して、この発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムの実施例を詳細に説明する。なお、以下では、本実施例で用いる主要な用語、ネットワーク攻撃防御システムの概要および特徴、中継装置の構成および処理、本実施例の効果を順に説明し、最後に本実施例に対する種々の変形例を説明する。

【実施例】

【００３０】

[用語の説明]

まず最初に、本実施例で用いる主要な用語を説明する。本実施例で用いる「容疑シグネチャ」とは、攻撃容疑のあるパケット（攻撃容疑パケット）を制限するためのシグネチャであり、具体的には、通過が制限される攻撃容疑パケットの特徴を示す属性（例えば、宛先ＩＰアドレス、プロトコル、宛先ポート番号など）や制限内容（例えば、特定のパケットが流入するときの帯域を制限するための制限情報など）を規定して構成される。

【００３１】

また、本実施例で用いる「正規シグネチャ」とは、容疑シグネチャに該当するパケットのなかから攻撃とはみなされない正規パケット（正規ユーザの通信パケットである正規パケット）の通過を許可するためのシグネチャであり、具体的には、通過が許可される正規パケットの特徴を示す属性（例えば、送信元ＩＰアドレス、サービスタイプ、宛先ＩＰアドレス、プロトコル、宛先ポート番号など）を規定して構成される。

【００３２】

また、本実施例で用いる「不正シグネチャ」とは、不正トラヒックに含まれる不正パケット（不正トラヒック条件を満たすパケット）を制限するためのシグネチャであり、具体的には、不正パケットの送信元ＩＰアドレス等を規定して構成される。

【００３３】

また、本実施例で用いる「識別情報（特許請求の範囲に記載の「生成識別情報」に対応する）」とは、上記したシグネチャの生成を一意に識別するための情報であり、具体的には、シグネチャの生成元である中継装置を一意に識別するための識別子（例えば、エンジンタイプ、エンジンＩＤおよびノードＩＤからなる識別子）および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子（例えば、シーケンシャルに付与される生成番号）から構成される。

【００３４】

また、本実施例で用いる「下流ノード（特許請求の範囲に記載の「中継元情報」に対応する）」とは、上記したシグネチャを隣接する中継装置から受信して他の隣接する中継装置に送信した中継装置において、当該シグネチャの直前の中継元である隣接中継装置（すなわち、どの中継装置からシグネチャを受信したか）を特定するための情報であり、具体的には、隣接中継装置のアドレスを規定して構成される。

【００３５】

また、本実施例で用いる「上流ノード（特許請求の範囲に記載の「中継先情報」に対応する）」とは、上記したシグネチャを隣接する中継装置から受信して他の隣接する中継装置に送信した中継装置において、当該シグネチャの直後の中継先である隣接中継装置（すなわち、どの中継装置に対してシグネチャを送信したか）を特定するための情報であり、具体的には、隣接中継装置のアドレスを規定して構成される。なお、シグネチャの中継元（下流ノード）は常に一つであるが、中継先（上流ノード）は複数になり得る。

【００３６】

[システムの概要および特徴]

次に、図１を用いて、本実施例に係るネットワーク攻撃防御システムの概要および特徴

を説明する。図１は、本実施例に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

【００３７】

同図に示すように、このネットワーク攻撃防御システム１００は、ネットワーク上に複数の中継装置１０を備えて構成される。また、このネットワーク上には、ＤｏＳ攻撃やＤＤｏＳ攻撃の対象となるコンピュータとしてのサーバ２０や、かかるＤｏＳ攻撃やＤＤｏＳ攻撃を行い得るコンピュータとしての通信端末３０が接続されている。なお、以下では、図示した中継装置１０の各々を区別する場合には、それぞれ中継装置１０－１～中継装置１０－７とし、サーバ２０の各々を区別する場合には、サーバ２０－１またはサーバ２０－２とし、通信端末３０の各々を区別する場合には、通信端末３０－１～通信端末３０－５として記載する。

【００３８】

ここで、中継装置１０の原則的な機能を最初に説明すると、中継装置１０は、通信端末３０のうち少なくとも１つ以上の通信端末３０がネットワーク上のサーバ２０に対してＤｏＳ攻撃またはＤＤｏＳ攻撃を行っていることを検出した場合に、パケットの通過を制御するためのシグネチャ（容疑シグネチャや不正シグネチャ）を生成するとともに、パケットの通過を許可するための正規シグネチャを生成する。そして、中継装置１０は、自ら生成したシグネチャ（容疑シグネチャ、不正シグネチャおよび正規シグネチャ）をシグネチャリストに登録する。

【００３９】

また、中継装置１０は、生成した容疑シグネチャ（さらには、正規シグネチャの生成に用いた正規条件）を隣接中継装置に送信する。さらに、中継装置１０は、容疑シグネチャの生成直後だけでなく、送信ミスや内容更新等に起因して容疑シグネチャを再送信する必要が生じた場合にも、容疑シグネチャ等を改めて隣接中継装置に送信する。

【００４０】

その一方で、中継装置１０は、隣接中継装置から容疑シグネチャ等を受信した場合には、原則として、正規条件に基づいて正規シグネチャを生成するとともに、受信した容疑シグネチャおよび生成した正規シグネチャをシグネチャリストに登録し、さらに、受信した容疑シグネチャおよび正規条件を他の隣接中継装置に送信する。なお、隣接中継装置について例を挙げると、図１において、中継装置１０－３における隣接中継装置は、中継装置１０－１、中継装置１０－２、中継装置１０－４および中継装置１０－７であり、中継装置１０－５および中継装置１０－６とは、隣接関係をもたない。また、この隣接関係は、物理的な隣接を意味するものではない。

【００４１】

このようにして、図１に示したネットワーク攻撃防御システム１００では、シグネチャを受信した各中継装置１０がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置１０が同様の容疑シグネチャや正規シグネチャをシグネチャリストに登録することになる。そして、各中継装置１０では、かかるシグネチャリストに登録されたシグネチャ基づいてパケットの通過を制御する。つまり、不正シグネチャや容疑シグネチャに該当するパケットについては、伝送帯域を制限して通過させるかもしくは廃棄し、正規シグネチャに該当するパケットやいずれのシグネチャにも該当しないパケットについては、伝送帯域を制限せずに通過を許可する。

【００４２】

ところで、本実施例における中継装置１０は、上記したような原則的な機能に加えて、隣接中継装置から受信したシグネチャがシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合に限り、シグネチャをシグネチャリストに登録するとともに隣接中継装置に送信するようにしている点に主たる特徴がある。つまり、隣接中継装置から受信したシグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことができるようにしている。

【００４３】

ここで、上記の主たる特徴を実現するために中継装置１０が備える特徴的な機能を説明すると、容疑のかかる攻撃を検出した中継装置１０では、攻撃容疑パケットを制限するための容疑シグネチャおよび容疑シグネチャの生成を一意に識別するための識別情報を生成する。そして、これら容疑シグネチャおよび識別情報を対応付けてシグネチャリストに登録するとともに、生成した容疑シグネチャ（さらには正規条件）および識別情報を隣接中継装置に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継先である隣接中継装置を特定するための上流ノードを容疑シグネチャおよび識別情報に対応付けてシグネチャリストに登録する。そして、容疑シグネチャを再送信する必要が生じた場合には、かかるシグネチャリストを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

【００４４】

一方、容疑シグネチャおよび識別情報を受信した中継装置１０では、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合には、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードを容疑シグネチャおよび識別情報に対応付けてシグネチャリストに登録する。

【００４５】

また、容疑シグネチャ等を受信した中継装置１０では、上記とは反対に、受信した容疑シグネチャの識別情報がシグネチャリストに既に登録されている場合には、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かをさらに判定する。そして、下流ノードが同一である場合には、シグネチャの再送信であるとして、受信した容疑シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている上流ノードが示す他の隣接中継装置にシグネチャを再送信する。

【００４６】

その一方、容疑シグネチャ等を受信した中継装置１０では、上記した判定において下流ノードが同一でない場合には、シグネチャの再送信でもないとして、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を隣接中継装置から受信した中継装置１０では、シグネチャリストに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。

【００４７】

以下に、図１を用いて、上記した主たる特徴が実現される具体例を説明する。同図に示すように、例えば、通信端末３０－４および通信端末３０－５がサーバ２０－１に対するＤｏＳ攻撃を行っており、中継装置１０－１が容疑のかかる攻撃を検出したとすると、中継装置１０－１は、攻撃容疑パケットを制限するための容疑シグネチャおよび識別情報を生成し、これら容疑シグネチャおよび識別情報を対応付けてシグネチャリストに登録するとともに、生成した容疑シグネチャ（さらには正規条件）および識別情報を隣接中継装置である中継装置１０－２および中継装置１０－３に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継装置１０－２および中継装置１０－３のアドレスを上流ノードとしてシグネチャリストに登録する（図１の（１）および（２）参照）。

【００４８】

一方、中継装置１０－２および中継装置１０－３は、中継装置１０－１から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定するが、ここでは、識別情報が未だ登録されていないので、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。つまり、中継装

置１０－２は、中継装置１０－４に容疑シグネチャおよび識別情報を送信し、また、中継装置１０－３は、中継装置１０－４および中継装置１０－７に容疑シグネチャおよび識別情報を送信する（同図の（３）および（４）参照）。

【００４９】

さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継装置１０－２および中継装置１０－３は、下流ノードおよび上流ノードの情報をシグネチャリストに登録する。つまり、中継装置１０－２は、中継装置１０－１のアドレスを下流ノードとして、中継装置１０－４のアドレスを上流ノードとしてシグネチャリストに登録し、また、中継装置１０－３は、中継装置１０－１のアドレスを下流ノードとして、中継装置１０－４および中継装置１０－７のアドレスを上流ノードとしてシグネチャリストに登録する。

【００５０】

そして、中継装置１０－７は、中継装置１０－３から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報は自己のシグネチャリストに未だ登録されていないので、上記した中継装置１０－２および中継装置１０－３と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するが、隣接中継装置がないので、当該容疑シグネチャおよび識別情報を隣接中継装置に送信することはしない。さらに、中継装置１０－７は、上流ノードは登録しないが、中継装置１０－３のアドレスを下流ノードとしてシグネチャリストに登録する（同図の（５）参照）。

【００５１】

その一方、中継装置１０－４は、例えば、中継装置１０－２から中継装置１０－３よりも先に容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに未だ登録されていないので、上記した中継装置１０－２および中継装置１０－３と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置となる中継装置１０－３、中継装置１０－５および中継装置１０－６に送信する。さらに、中継装置１０－４は、中継装置１０－２のアドレスを下流ノードとしてシグネチャリストに登録するとともに、中継装置１０－３、中継装置１０－５および中継装置１０－６のアドレスを上流ノードとしてシグネチャリストに登録する（図（６）および（７）参照）。

【００５２】

そして、中継装置１０－５および中継装置１０－６は、中継装置１０－４から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報が自己のシグネチャリストに未だ登録されていないので、上記した中継装置１０－７と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するが、隣接中継装置がないので、当該容疑シグネチャおよび識別情報を隣接中継装置に送信することはしない。さらに、中継装置１０－５および中継装置１０－６は、上流ノードは登録しないが、中継装置１０－４のアドレスを下流ノードとしてシグネチャリストに登録する（同図の（８）参照）。

【００５３】

ところで、中継装置１０－４は、上記した例によって、中継装置１０－２から容疑シグネチャおよび識別情報を受信した後、中継装置１０－３からも同一の容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されており、かつ、識別情報に対応付けて登録されている下流ノード（中継装置１０－２）が現に受信したシグネチャの下流ノード（中継装置１０－３）と同一でないので、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである中継装置１０－２に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を中継装置１０－４から受信した中継装置１０－３では、シグネチャリストに記憶された当該シグネチャの上流ノードから中継装置１０－４のアドレスを削除する。

【００５４】

また、中継装置１０－３は、上記した例によって、中継装置１０－４からも同一の容疑

シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されており、かつ、識別情報に対応付けて登録されている下流ノード（中継装置１０－１）が現に受信したシグネチャの下流ノード（中継装置１０－４）と同一でないので、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである中継装置１０－４に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を中継装置１０－３から受信した中継装置１０－４では、シグネチャリストに記憶された当該シグネチャの上流ノード（中継装置１０－３、中継装置１０－５および中継装置１０－６のアドレス）から中継装置１０－３のアドレスを削除する。

【００５５】

さらに、中継装置１０－４は、上記した例によって、中継装置１０－２から容疑シグネチャおよび識別情報を受信した後、同じく中継装置１０－２から同一の識別情報からなる容疑シグネチャを受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているが、識別情報に対応付けて登録されている下流ノード（中継装置１０－２）が現に受信したシグネチャの下流ノード（中継装置１０－２）と同一であるので、シグネチャの再送信であるとして、受信した容疑シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている上流ノード（中継装置１０－５および中継装置１０－６のアドレス）が示す中継装置１０－５および中継装置１０－６に容疑シグネチャを再送信する。

【００５６】

以上のように、図１に示したネットワーク攻撃防御システムでは、隣接中継装置から受信したシグネチャがシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合に限り、シグネチャをシグネチャリストに登録するとともに隣接中継装置に送信するようにすることで、上記した例で言えば、中継装置１０－４や中継装置１０－３においてシグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

【００５７】

なお、中継装置１０は、攻撃を防御しながらパケットを中継するための装置であり、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、中継装置１０は、中継装置１０等を管理するための管理用ネットワークに接続されていてもよく、シグネチャは、管理用ネットワークを介して送受されてもよい。さらに、中継装置１０が送信するシグネチャは、容疑シグネチャだけに限定されず、中継装置１０は、他のシグネチャを送信してもよく、容疑シグネチャに加えて他のシグネチャを送信するようにしてもよい。

【００５８】

[中継装置の構成]

次に、図２を用いて、図１に示した中継装置１０の構成を説明する。図２は、中継装置１０の構成を示すブロック図である。同図に示すように、この中継装置１０は、ネットワークインタフェース１１と、パケット取得部１２と、攻撃検出部１３（並びに攻撃容疑検出条件テーブル１３ａ、不正トラヒック検出条件テーブル１３ｂおよび正規条件テーブル１３ｃ）と、シグネチャ通信部１４と、識別情報判定部１５と、フィルタ部１６（並びにシグネチャリスト１６ａ）とを備えて構成される。

【００５９】

また、中継装置１０は、ＣＰＵ（Central Processing Unit）やメモリ、ハードディスク等を有しており、パケット取得部１２、攻撃検出部１３、シグネチャ通信部１４、識別情報判定部１５およびフィルタ部１６は、ＣＰＵによって処理されるプログラムのモジュールであってもよい。また、このプログラムのモジュールは、１つのＣＰＵで処理されてもよく、複数のＣＰＵに分散して処理されてもよい。さらに、中継装置１０には、Ｌｉｎｕｘ等の汎用ＯＳをインストールしておき、汎用ＯＳに具備されるパケットフィルタをフ

ィルタ部１６として機能させてもよい。

【００６０】

なお、攻撃検出部１３は特許請求の範囲に記載の「シグネチャ生成手段」に対応し、シグネチャ通信部１４は同じく「シグネチャ通信手段」に対応し、識別情報判定部１５は同じく「シグネチャ登録判定手段」に対応し、シグネチャリスト１６ａは同じく「シグネチャ記憶手段」に対応する。

【００６１】

図２において、ネットワークインタフェース部１１は、ネットワークと接続されている通信機器との間でパケットを送受する手段であり、具体的には、ＬＡＮ（Local Area Network）またはＷＡＮ（Wide Area Network）などのネットワークと接続するためのネットワーク接続カード等によって構成される。なお、図２には示していないが、キーボードやマウス、マイクなど、ネットワーク管理者から各種の情報や指示の入力を受付ける入力手段や、モニタ（若しくはディスプレイ、タッチパネル）やスピーカなど、各種の情報を出力する出力手段を備えて中継装置１０を構成するようにしてもよい。

【００６２】

パケット取得部１２は、ネットワークインタフェース部１１が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部１３およびパケット数判定部１５ａに提供する処理部である。

【００６３】

攻撃検出部１３は、パケット取得部１２によって提供された統計情報に基づいて、攻撃の検出および攻撃の分析を行う処理部であり、図２に図示するように、攻撃容疑検出条件テーブル１３ａ、不正トラヒック検出条件テーブル１３ｂおよび正規条件テーブル１３ｃにそれぞれ接続される。ここで、各テーブル１３ａ～１３ｃに記憶される情報を具体的に説明した後に、攻撃検出部１３による処理内容を説明する。

【００６４】

図３は、攻撃容疑検出条件テーブル１３ａに記憶される情報、より詳細には、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用される「攻撃容疑検出条件」の一例を示す図である。同図に示すように、攻撃容疑検出条件は、検出属性、検出閾値および検出間隔の組合せからなる複数組（ここでは３組）のレコードで構成され、かかる攻撃容疑検出条件の各レコードの内のいずれかのレコードの条件にトラヒックが一致した場合に、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。なお、番号はレコードを特定するために便宜上使用されるものである。

【００６５】

攻撃容疑検出条件の「検出属性」には、例えば、ＩＰパケットに含まれるＩＰヘッダ部の属性や、ＩＰパケットのペイロード部に含まれるＴＣＰヘッダ部またはＵＤＰヘッダ部の属性が指定される。具体的には、図３において、番号１のレコードの検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.1/32」であり（dst=192.168.1.1/32）、ＩＰの上位層（ＴＣＰまたはＵＤＰ）のプロトコル種別を示す「Protocol（プロトコル）」が「ＴＣＰ」であり（Protocol=TCP）、かつ、ＩＰの上位層プロトコルがどのアプリケーションの情報であるかを示す「Destination Port（宛先ポート番号）」が「８０」である（Port=80）という属性値の組で指定される。

【００６６】

また、番号２のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.2/32」であり（dst=192.168.1.2/32）、かつ、「Protocol（プロトコル）」が「ＵＤＰ（User Datagram protocol）」である（Protocol=UDP）という属性値の組で指定される。同様に、番号３のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.0/24」という属性で指定される。

【００６７】

攻撃容疑検出条件の「検出閾値」は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を指定し

たものであり、攻撃容疑検出条件の「検出間隔」は、同じく最低の連続時間を指定したものである。なお、図３には示していないが、検出属性においては、「Destination IP Address（宛先ＩＰアドレス）」の値を無条件（ａｎｙ）とし、かつ、ＩＰの上位層のプロトコル種別を示す「Protocol（プロトコル）」が「ＩＣＭＰ（Internet Control Message Protocol）」となる属性値の組を指定するようにしてもよい。

【００６８】

図４は、不正トラヒック検出条件テーブル１３ｂに記憶される情報、より詳細には、攻撃容疑パケットのトラヒックから不正トラヒックを検出するために用いられる「不正トラヒック条件」の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のＤＤｏＳ攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。なお、番号はレコード（パターン）を特定するために便宜上使用されるものである。

【００６９】

具体的には、番号１の不正トラヒック条件は、「伝送帯域Ｔ１Ｋｂｐｓ以上、パケットがＳ１秒以上連続送信されている」というトラヒックパターンを示している。また、番号２の不正トラヒック条件は、「伝送帯域Ｔ２Ｋｂｐｓ以上、ＩＣＭＰ（Internet Control Message Protocol）上のエコー応答（Echo Reply）メッセージのパケットがＳ２秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号３の不正トラヒック条件は、「伝送帯域Ｔ３Ｋｂｐｓ以上、データが長すぎるためパケットに含まれるデータは複数ＩＰパケットに分割して送信していることを示すフラグメントパケットがＳ３秒以上連続送信されている」というトラヒックパターンを示している。

【００７０】

図５は、正規条件テーブル１３ｃに記憶される情報、より詳細には、正当な利用者が利用している通信端末３０から送信されるパケットを表す「正規条件」の一例を示す図である。同図に示すように、正規条件は、ＩＰパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード（パターン）を特定するために便宜上使用されるものである。

【００７１】

具体的には、番号１のレコードの検出属性は、ＩＰの「Source IP Address（送信元ＩＰアドレス）」が「172.16.10.0/24」であることを指定し（src=172.16.10.0/24）、番号２のレコードの検出属性はＩＰ上のサービス品質を示す「Type of Service（サービスタイプ）」が「（１６進で）０１」であることを指定している（TOS=0x01）。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ２０等の送信元ＩＰアドレスが設定され、サーバ２０が収容されているＬＡＮの所有者が正規ユーザであると認識しているネットワークの送信元ＩＰアドレスなどが設定される。

【００７２】

図２の説明に戻ると、攻撃検出部１３は、パケット取得部１２によって提供された統計情報に基づいて攻撃の検出を検出した場合に、攻撃容疑トラヒックの通信パケット（攻撃容疑パケット）を制限するための容疑シグネチャを生成する。具体的には、攻撃検出部１３は、図３に示した攻撃容疑検出条件に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、各レコードの内のいずれかのレコードに合致した場合には、このトラヒックを攻撃容疑トラヒックとして検出し、このときに検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を容疑シグネチャとして生成する。

【００７３】

また、攻撃検出部１３は、攻撃を検出した場合に、容疑シグネチャとともに正規シグネチャを生成する。具体的には、図５に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのＡＮＤ条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケッ

トを許可するために用いられるシグネチャであるが、例えば、図３および図５の例を用いて説明すると、図３における番号１のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32，Protocol=TCP，Port=80]となり、図５において、正規シグネチャは、[src=172.16.10.24，dst=192.168.1.1/32，Protocol=TCP，Port=80]および[TOS=0x01，dst=192.168.1.1/32，Protocol=TCP，Port=80]となる。

【００７４】

さらに、攻撃検出部１３は、図４に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元ＩＰアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

【００７５】

上述してきた攻撃検出部１３によって生成された容疑シグネチャ、正規シグネチャおよび不正シグネチャは、シグネチャリスト１６ａ（図６参照）に登録される。そして、攻撃検出部１３は、各シグネチャの生成を一意に識別するための識別情報を生成し、この識別情報とともにシグネチャをシグネチャリスト１６ａに登録する。

【００７６】

ここで、図７を参照して、シグネチャに付与される識別情報を説明する。図７は、シグネチャに付与される識別情報の例を示す図であるが、同図に示すように、攻撃検出部１３は、シグネチャの生成元である中継装置１０を一意に識別するための識別子（すなわち、エンジンタイプ、エンジンＩＤおよびノードＩＤからなる識別子）および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子（例えば、シーケンシャルに付与される生成番号）から構成される識別情報を生成する。

【００７７】

図２において、シグネチャ通信部１４は、攻撃検出部１３が生成したシグネチャ等を隣接中継装置に送信するとともに、隣接中継装置から送信されたシグネチャを受信し、また、隣接中継装置から受信したシグネチャをシグネチャリスト１６ａに登録し、さらに、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理部である。

【００７８】

具体的には、シグネチャ通信部１４は、攻撃検出部１３によってシグネチャおよび識別情報がシグネチャリスト１６ａに登録されると、登録されたシグネチャ等を識別情報とともに隣接中継装置に送信する。さらに、シグネチャ通信部１４は、かかるシグネチャおよび識別情報の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト１６ａに登録する（図６参照）。そして、シグネチャ通信部１４は、容疑シグネチャ等を再送信する必要が生じた場合には、かかるシグネチャリスト１６ａを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

【００７９】

また、シグネチャ通信部１４は、隣接中継装置から受信したシグネチャをシグネチャリスト１６ａに登録する処理および他の隣接中継装置に送信する処理を行うが、かかる処理は、以下に説明する識別情報判定部１５による判定結果に従って実行される。

【００８０】

識別情報判定部１５は、シグネチャ通信部１４によって隣接中継装置からシグネチャを受信した場合に、受信したシグネチャの識別情報がシグネチャリスト１６ａに既に登録されているか否かを判定する。そして、未だ登録されていないと識別情報判定部１５が判定した場合には、上記のシグネチャ通信部１４は、受信したシグネチャおよび識別情報をシグネチャリスト１６ａに登録するとともに、当該シグネチャおよび識別情報を隣接中継装置に送信する。さらに、シグネチャ通信部１４は、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト１６ａに登録する（図６参照）。

【００８１】
これとは反対に、受信したシグネチャの識別情報がシグネチャリスト１６ａに既に登録されている場合には、識別情報判定部１５は、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かをさらに判定する。そして、下流ノードが同一であると識別情報判定部１５が判定した場合には、上記のシグネチャ通信部１４は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト１６ａに上書き登録するとともに、シグネチャリスト１６ａに登録されている上流ノードが示す他の隣接中継装置にシグネチャを再送信する。
【００８２】
さらに、上記した判定において、下流ノードが同一でないと識別情報判定部１５が判定した場合には、上記のシグネチャ通信部１４は、シグネチャの再送信でもないとして、受信した容疑シグネチャをシグネチャリスト１６ａに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。その一方、シグネチャ通信部１４は、かかる既登録通知を隣接中継装置から受信した場合には、シグネチャリスト１６ａに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。
【００８３】
図２において、フィルタ部１６は、ネットワークインタフェース部１１が受信したパケットを受け入れて、シグネチャリスト１６ａに基づいてパケットの通過（ネットワークインタフェース部１１からのパケットの出力）を制御する処理部である。具体的には、入力されたパケットについて、シグネチャリスト１６ａに登録された「不正シグネチャ」、「正規シグネチャ」、「容疑シグネチャ」のいずれかに該当するか（もしくはいずれにも該当しないか）を判別した上で、該当するシグネチャに基づいてパケットの通過を制御する。
【００８４】
より詳細には、フィルタ部１６は、不正シグネチャに該当するパケットは、不正なパケットを処理するための不正キューに入力し、容疑シグネチャに該当するパケットは、容疑ユーザ用の容疑キューに入力し、正規シグネチャに該当するパケットまたはいずれのシグネチャにも該当しないパケットは、正規ユーザ用の正規キューに入力する。その上で、フィルタ部１６は、正規キューに入力されたパケットについては、伝送帯域を制限せずにネットワークインタフェース部１１から出力し、容疑キューおよび不正キューに入力されたパケットについては、それぞれのシグネチャ（条件を満たすとして選択されたシグネチャ）が示す伝送帯域制限値に従って制限して出力する。
【００８５】
なお、フィルタ部１６は、シグネチャリスト１６ａに登録されたシグネチャの検出属性等が所定の解除判断基準を満たした場合には、この所定の解除判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいてパケットの通過を制御する処理を停止する。
【００８６】
[攻撃容疑パケット検出時の処理]
続いて、図８を参照して、上記した中継装置１０による攻撃容疑パケット検出時の動作処理を説明する。図８は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。
【００８７】
同図に示すように、中継装置１０の攻撃検出部１３は、図３に示した攻撃容疑検出条件テーブル１３ａに基づいて攻撃容疑トラヒックを検出すると（ステップＳ１）、容疑シグネチャおよび正規シグネチャを生成する（ステップＳ２）。
【００８８】
そして、攻撃検出部１３は、各シグネチャの生成を一意に識別するための識別情報を生

成し（ステップＳ３）、この識別情報とともに容疑シグネチャおよび正規シグネチャをフィルタ部１６のシグネチャリスト１６ａに登録する（ステップＳ４）。さらに、シグネチャ通信部１４は、攻撃検出部１３が生成したシグネチャ等（本実施例では、容疑シグネチャおよび正規条件）を識別情報とともに隣接中継装置に送信する（ステップＳ５）。

【００８９】

なお、シグネチャ通信部１４は、上記したステップＳ４によるシグネチャ等の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャリスト１６ａに登録する。そして、シグネチャ通信部１４は、容疑シグネチャ等を再送信する必要が生じた場合には、かかるシグネチャリスト１６ａを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

【００９０】

[シグネチャ受信時の処理]

続いて、図９を参照して、上記した中継装置１０によるシグネチャ受信時の動作処理を説明する。図９は、シグネチャ受信時の処理手順を示すフローチャートである。

【００９１】

同図に示すように、中継装置１０のシグネチャ通信部１４が、隣接中継装置から送信されたシグネチャ等（本実施例では、容疑シグネチャおよび正規条件）を受信すると（ステップＳ１１）、識別情報判定部１５は、受信したシグネチャの識別情報がフィルタ部１６のシグネチャリスト１６ａに既に登録されているか否かを判定し（ステップＳ１２）、さらに、かかる識別情報がシグネチャリスト１６ａに既に登録されている場合には（ステップＳ１２肯定）、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かも判定する（ステップＳ１３）。

【００９２】

かかる判定において、識別情報がシグネチャリスト１６ａに既に登録されているおり、かつ、下流ノードが同一でないと識別情報判定部１５が判定した場合には（ステップＳ１２肯定かつステップＳ１３否定）、シグネチャ通信部１４は、受信した容疑シグネチャをシグネチャリスト１６ａに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する（ステップＳ１３１）。なお、かかる既登録通知を隣接中継装置から受信した中継装置１０では、シグネチャリスト１６ａに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。

【００９３】

これとは反対に、受信したシグネチャの識別情報がシグネチャリスト１６ａに未だ登録されていないと識別情報判定部１５が判定した場合には（ステップＳ１２否定）、シグネチャ通信部１４は、受信したシグネチャおよび識別情報をフィルタ部１６のシグネチャリスト１６ａに登録し（ステップＳ１４）、攻撃検出部１３は、シグネチャ通信部１４が受信した正規条件に基づいて正規シグネチャを生成するとともに（ステップＳ１５）、正規シグネチャをシグネチャリスト１６ａに登録する（ステップＳ１６）。

【００９４】

さらに、シグネチャ通信部１４は、シグネチャリスト１６ａに登録した容疑シグネチャおよび識別情報（さらには、正規シグネチャの生成に用いた正規条件）を隣接中継装置に送信する（ステップＳ１７）。なお、シグネチャ通信部１４は、このステップＳ１７によるシグネチャ等の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト１６ａに登録する。

【００９５】

ところで、上記したステップＳ１３の判定において、受信したシグネチャの識別情報がシグネチャリスト１６ａに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であると識別情報判定部１５が

判定した場合には（ステップＳ１３肯定）、シグネチャ通信部１４は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト１６ａに上書き登録するとともに（ステップＳ１３２）、攻撃検出部１３は、シグネチャ通信部１４が受信した正規条件に基づいて正規シグネチャを再生成するとともに（ステップＳ１３３）、正規シグネチャをシグネチャリスト１６ａに上書き登録する（ステップＳ１３４）。さらに、シグネチャ通信部１４は、シグネチャリスト１６ａに登録されている上流ノードが示す他の隣接中継装置に、容疑シグネチャおよび識別情報（さらには、正規シグネチャの生成に用いた正規条件）を再送信する（ステップＳ１３５）。

【００９６】

なお、上記では、シグネチャの再送信であると判定された場合（受信したシグネチャの識別情報がシグネチャリスト１６ａに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一である場合）に、容疑シグネチャの上書き登録、正規シグネチャの再生成および上書き登録（ステップＳ１３２～Ｓ１３４）を行う場合を説明したが、本発明は必ずしもこれに限定されるものではなく、これらの処理（ステップＳ１３２～Ｓ１３４）を省いて、容疑シグネチャ、識別情報および正規条件の再送信（ステップＳ１３５）のみを行うようにしてもよい。

【００９７】

[不正パケット検出時の処理]

続いて、図１０を参照して、上記した中継装置１０による不正パケット検出時の動作処理を説明する。図１０は、不正パケット検出時の処理手順を示すフローチャートである。

【００９８】

同図に示すように、中継装置１０の攻撃検出部１７が、図４に示した不正トラヒック条件に基づいて不正トラヒックを検出すると（ステップＳ２１）、不正シグネチャを生成する（ステップＳ２２）。そして、攻撃検出部１７は、生成した不正シグネチャをフィルタ部１６のシグネチャリスト１６ａに登録する（ステップＳ２３）。

【００９９】

[パケット制御時の処理]

続いて、図１１を参照して、上記した中継装置１０によるパケット制御時の動作処理を説明する。図１１は、パケット制御時の処理手順を示すフローチャートである。

【０１００】

同図に示すように、フィルタ部１６は、ネットワークインタフェース部１１からパケットが入力されると（ステップＳ３１肯定）、シグネチャリスト１６ａに登録された不正シグネチャに合致するか否かを判断する（ステップＳ３２）。そして、不正シグネチャに合致した場合には（ステップＳ３２肯定）、フィルタ部１６は、不正なパケットを処理するための不正キューにパケットを入力する（ステップＳ３３）。

【０１０１】

これとは反対に、不正シグネチャに合致しない場合には（ステップＳ３２否定）、フィルタ部１６は、入力されたパケットが、シグネチャリスト１６ａに登録された正規シグネチャに合致するか否かを判断する（ステップＳ３４）。そして、正規シグネチャに合致した場合には（ステップＳ３４肯定）、フィルタ部１６は、正規なユーザ用の正規キューにパケットを入力する（ステップＳ３５）。

【０１０２】

さらに、この正規シグネチャにも合致しない場合には（ステップＳ３４否定）、フィルタ部１６は、入力されたパケットが、シグネチャリスト１６ａに登録された容疑シグネチャに合致するか否かを判断する（ステップＳ３６）。そして、容疑シグネチャに合致した場合には（ステップＳ３６肯定）、フィルタ部１６は、容疑ユーザ用の容疑キューにパケットを入力する（ステップＳ３７）。これとは反対に、容疑シグネチャに合致しない場合には（ステップＳ３６否定）、フィルタ部１６は、正規キューにパケットを入力する（ステップＳ３８）。

【０１０３】

そして、フィルタ部１６は、それぞれのキューにあるパケットについて、正規キューであれば、伝送帯域を制限せずにネットワークインタフェース部１１から出力し、容疑キューおよび不正キューであれば、それぞれのシグネチャが示す伝送帯域制限値に従って制限して出力する。なお、不正シグネチャ、正規シグネチャ、容疑シグネチャの各シグネチャは、それぞれシグネチャリスト１６ａに複数登録されてもよい。また、登録されたシグネチャの検出属性等が所定の判断基準を満たした場合に、フィルタ部１６は、所定の判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいたパケットの通過を制御する処理を停止する。

【０１０４】

[実施例の効果]

上述してきたように、上記の実施例によれば、隣接中継装置から受信したシグネチャが既に登録されているか否かを判定して、未だ登録されていないシグネチャのみをシグネチャリスト１６ａに登録するとともに隣接中継装置に送信するので、シグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

【０１０５】

また、上記の実施例によれば、シグネチャの生成を一意に識別するための識別情報を各シグネチャに対応付けて管理するので、シグネチャの具体的な内容にまで踏み込むことなく、識別情報のみからシグネチャが既に登録されているか否かを判定することが可能になる。さらに、シグネチャの内容が同一であっても識別情報（生成元）が異なっていれば、未だ登録されていないシグネチャであるとしてシグネチャリスト１６ａに登録するとともに隣接中継装置に送信するので、生成元となる各中継装置の性能違い（例えば、攻撃検出や防御解除に係るアルゴリズムの違いなど）が尊重され、安全性の高いパケット制御を行うことが可能になる。

【０１０６】

また、上記の実施例によれば、攻撃容疑パケットを検出すると、容疑シグネチャおよび識別情報を生成し、これらシグネチャおよび識別情報を隣接中継装置に送信するとともに、中継先である隣接中継装置を特定するための上流オード、識別情報および容疑シグネチャをシグネチャリスト１６ａに対応付けて登録するので、シグネチャに対して確実に識別情報を付与することが可能になる。さらに、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリスト１６ａに登録された上流ノード、識別情報およびシグネチャを参照することで、同一の識別情報が付与されたシグネチャを同一の中継先に対して確実に再送信することが可能になる。

【０１０７】

また、上記の実施例によれば、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト１６ａに未だ登録されていない場合には、これを他の隣接中継装置に送信するとともに、シグネチャの直前の中継元である隣接中継装置を特定するための下流ノード、シグネチャの直後の中継先である隣接中継装置を特定するための上流ノード、識別情報およびシグネチャをシグネチャリスト１６ａに対応付けて登録する（図６参照）。そして、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト１６ａに既に登録されている場合には、下流ノードが同一であるか否かをさらに判定し、これが同一である場合には、シグネチャをシグネチャリスト１６ａに上書き登録するとともに、シグネチャリスト１６ａに登録されている上流ノードが示す他の隣接中継装置にシグネチャを送信するので、送信ミスや内容更新等に起因してシグネチャが再送信されてきた場合でも、このシグネチャを留めることなく、中継先に対して確実に再送信することが可能になる。その一方、下流ノードが同一でない場合には、シグネチャの再送信でもないと判定される結果、シグネチャの重複登録や重複送信を確実に回避することが可能になる。

【０１０８】

また、上記の実施例によれば、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト１６ａに既に登録されており、かつ、下流ノードも同一でない場合には、シ

グネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。さらに、当該既登録通知を他の隣接中継装置から受信した場合には、シグネチャリスト１６ａに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。したがって、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリスト１６ａから削除された中継先に対してはシグネチャが送信されないことになり、シグネチャの再送信に際してもシグネチャの重複登録や重複送信を確実に回避することが可能になる。

【０１０９】

［他の実施例］

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。

【０１１０】

例えば、上記の実施例では、シグネチャの生成を一意に識別するための生成識別情報に基づいて重複登録を判定する場合を説明したが、本発明はこれに限定されるものではなく、生成元となる各中継装置の性能を無視し、シグネチャの内容が同一であるか否かによって重複登録を判定するようにしてもよい。さらには、生成元となる各中継装置の性能を考慮し、シグネチャの内容が同一であり、かつ、生成元の性能が同一であるか否かによって重複登録を判定するようにしてもよい。

【０１１１】

また、各中継装置１０は、受信した容疑シグネチャおよび識別情報を隣接中継装置に送信する前に、容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したか否かを判定するようにしてもよい。すなわち、所定の閾値を超過したと判定した場合に初めて（攻撃有りと判定した場合に初めて）、受信した容疑シグネチャを隣接中継装置に送信するようにしてもよい。例えば、図１に示した例で言えば、中継装置１０－４は、通信端末３０－１～通信端末３０－３によって攻撃がなされていないので、中継装置１０－２または中継装置１０－３から容疑シグネチャおよび識別情報を受信したとしても、所定の閾値を超過したと判定することはなく、容疑シグネチャを隣接中継装置となる中継装置１０－５や中継装置１０－６に送信しない。

【０１１２】

また、上記の実施例で図示した各装置（例えば、図１に例示した中継装置１０）の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、中継装置１０の分散・統合の具体的形態は図示のものに限られず、中継装置１０の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、中継装置１０にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【０１１３】

また、上記の実施例で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報（例えば、攻撃容疑検出条件テーブル、不正トラヒック検出条件テーブル、正規条件テーブルの内容等）については、特記する場合を除いて任意に変更することができる。

【０１１４】

なお、上記の実施例では、本発明を実現する各装置（例えば、中継装置１０）を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。すなわち、本実施例で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ

上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例に示したような中継装置用プログラムを格納したＣＤ－ＲＯＭを配布し、このＣＤ－ＲＯＭに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

【産業上の利用可能性】

【０１１５】

以上のように、本発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムは、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャリストに登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する場合に有用であり、特に、シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことに適する。

【図面の簡単な説明】

【０１１６】

【図１】ネットワーク攻撃防御システムの構成を示すシステム構成図である。

【図２】中継装置の構成を示すブロック図である。

【図３】攻撃容疑検出条件テーブルに記憶される情報の例を示す図である。

【図４】不正トラヒック検出条件テーブルに記憶される情報の例を示す図である。

【図５】正規条件テーブルに記憶される情報の例を示す図である。

【図６】シグネチャリストに記憶される情報の例を示す図である。

【図７】シグネチャに付与される識別情報の例を示す図である。

【図８】攻撃容疑パケット検出時の処理手順を示すフローチャートである。

【図９】シグネチャ受信時の処理手順を示すフローチャートである。

【図１０】不正パケット検出時の処理手順を示すフローチャートである。

【図１１】パケット制御時の処理手順を示すフローチャートである。

【図１２】従来技術に係るネットワーク攻撃防御システムを説明するための図である。

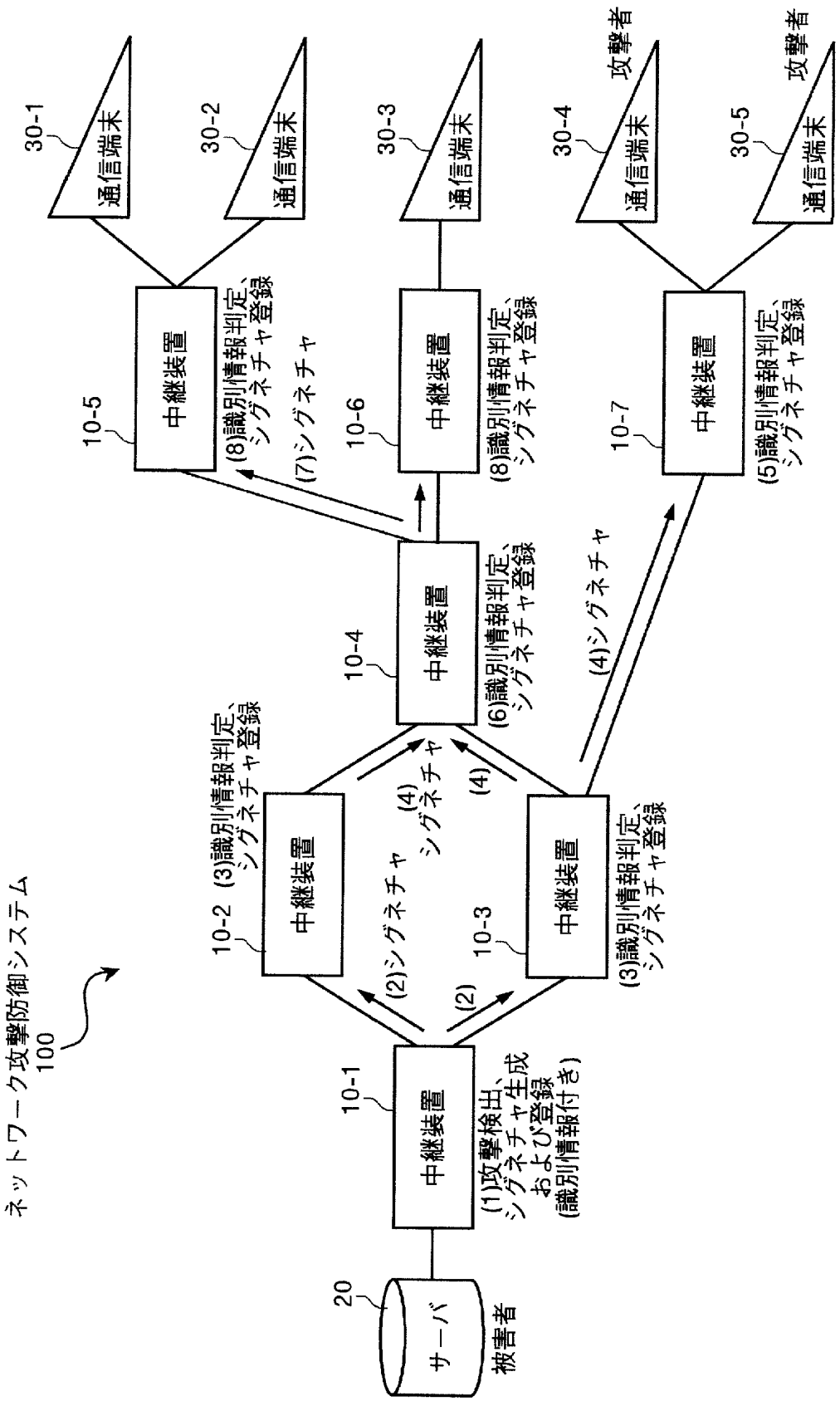
【図１３】従来技術に係るネットワーク攻撃防御システムを説明するための図である。

【符号の説明】

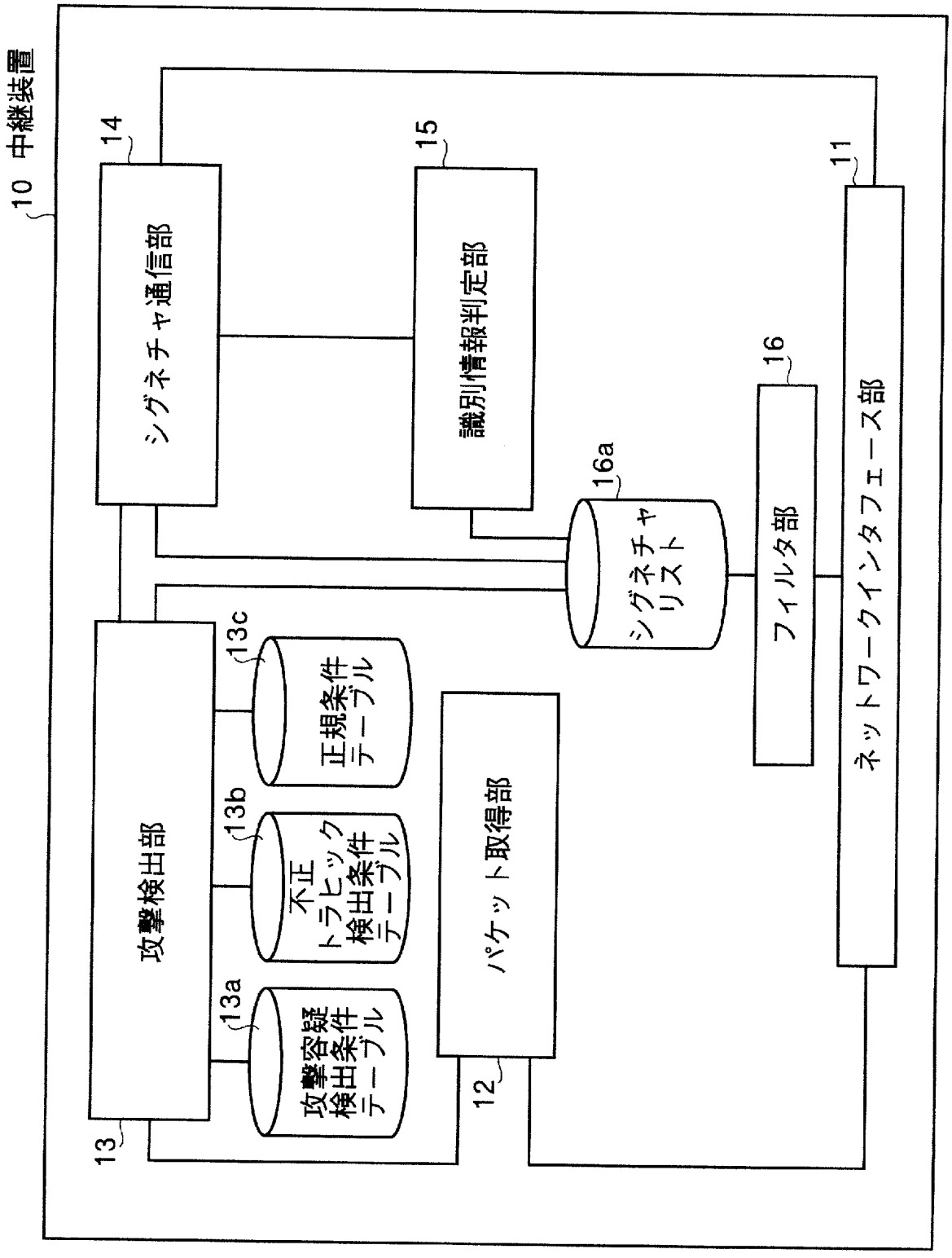
【０１１７】

１０　中継装置
１１　ネットワークインタフェース
１２　パケット取得部
１３　攻撃検出部
１４　シグネチャ通信部
１５　識別情報判定部
１６　フィルタ部
２０　サーバ
３０　通信端末
１００　ネットワーク攻撃防御システム

【書類名】図面
【図１】


ネットワーク攻撃防御システム
100
10-1
中継装置
(1)攻撃検出、
シグネチャ生成
および登録
(識別情報付き)
20
サーバ
被害者
(2)シグネチャ
(2)
10-2
中継装置
(3)識別情報判定、
シグネチャ登録
10-3
中継装置
(3)識別情報判定、
シグネチャ登録
(4)
シグネチャ
(4)シグネチャ
10-4
中継装置
(6)識別情報判定、
シグネチャ登録
10-5
中継装置
(8)識別情報判定、
シグネチャ登録
(7)シグネチャ
10-6
中継装置
(8)識別情報判定、
シグネチャ登録
10-7
中継装置
(5)識別情報判定、
シグネチャ登録
30-1
通信端末
30-2
通信端末
30-3
通信端末
30-4
攻撃者
通信端末
30-5
攻撃者
通信端末

【図２】


10 中継装置
14
シグネチャ通信部
15
識別情報判定部
11
16
16a
シグネチャリスト
フィルタ部
ネットワークインタフェース部
13
攻撃検出部
13c
正規条件テーブル
13b
不正トラヒック検出条件テーブル
13a
攻撃容疑検出条件テーブル
12
パケット取得部

【図３】

13a 攻撃容疑検出条件テーブル

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500Kbps	10秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300Kbps	10秒
3	{Dst=192.168.1.1/24}	1000Kbps	20秒
⋮			

【図４】

13b 不正トラヒック条件検出テーブル

番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
3	T3Kbps以上のフラグメントパケットが S3秒以上連続送信されている
⋮	

【図５】

13c 正規条件テーブル

番号	検出属性
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

【図６】

16a シグネチャリスト

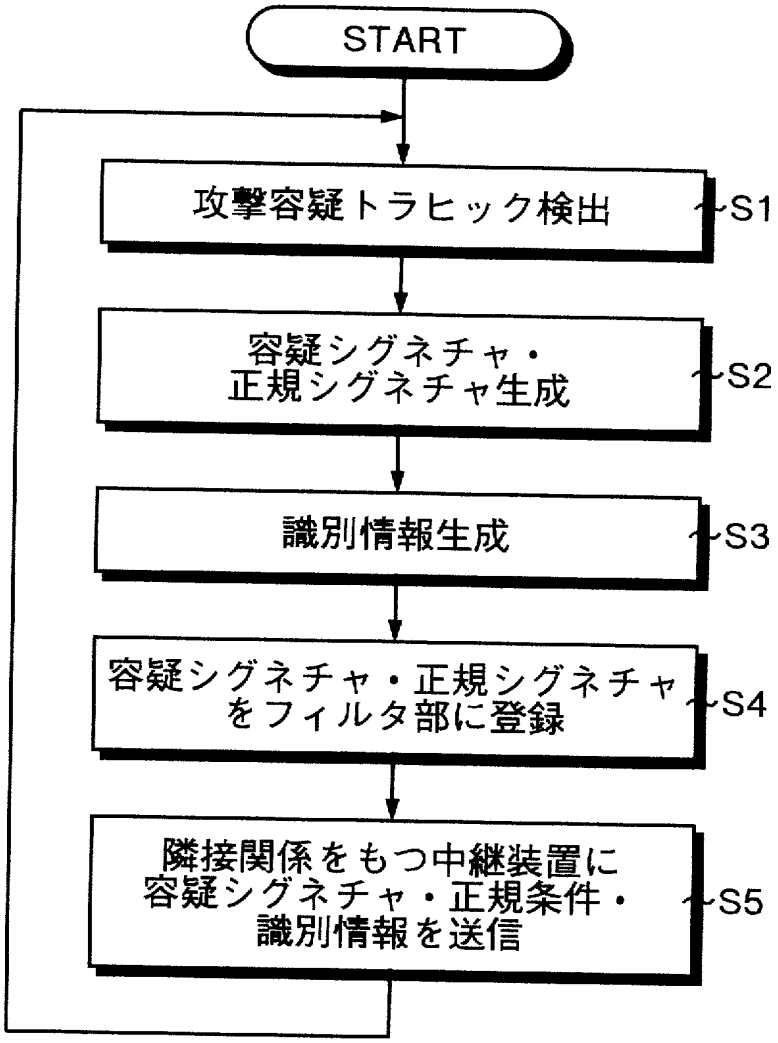
シグネチャ	識別情報	下流ノード	上流ノード
シグネチャA	(…,…,…,…)	中継装置 10-2	中継装置 10-5,10-6
シグネチャB	(…,…,…,…)	中継装置 10-3	中継装置 10-5,10-6
⋮	⋮	⋮	⋮

【図７】

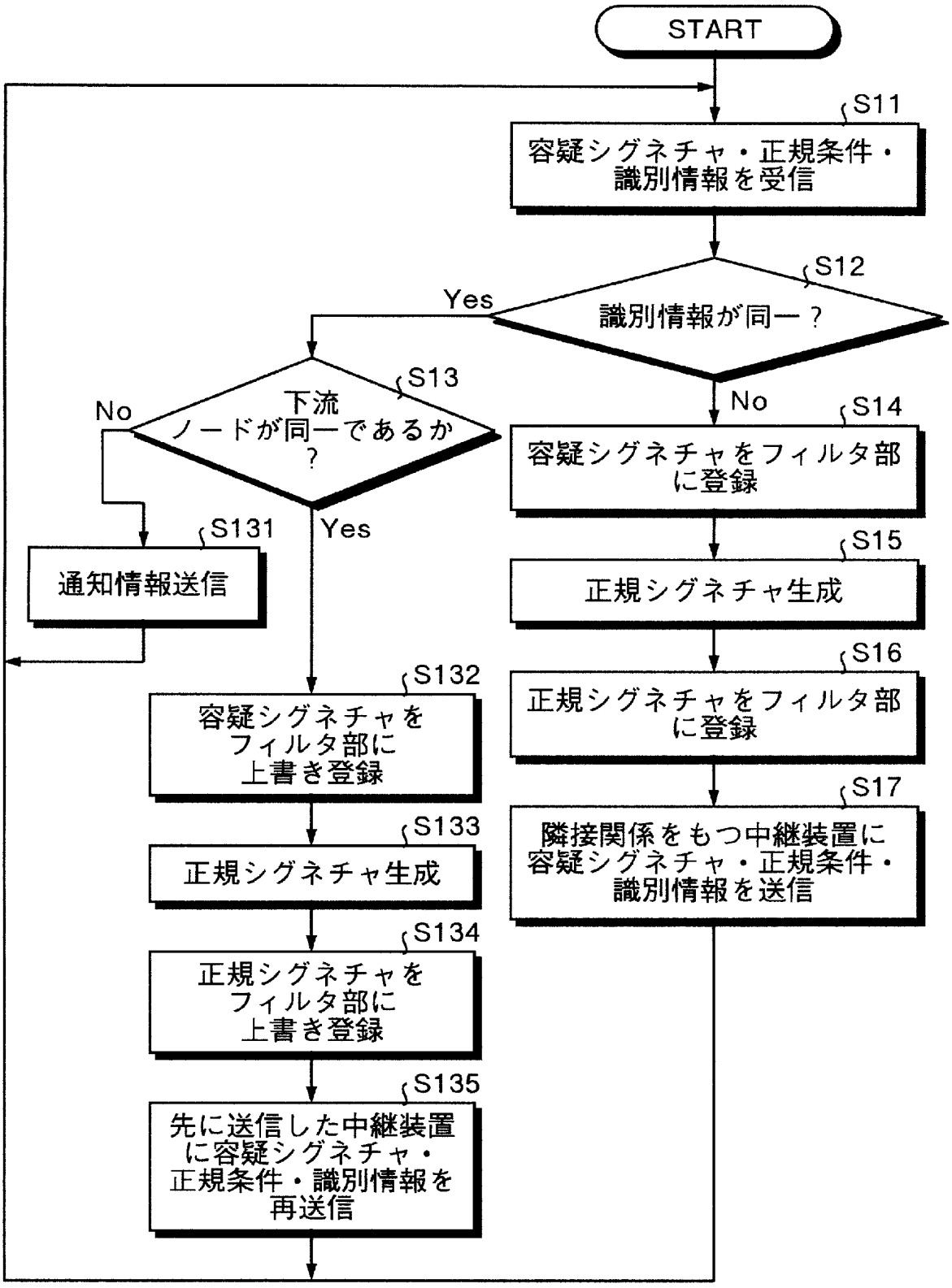
識別情報:{Local Alert ID,Engine-type,Engine-ID,Node-ID}

- Local Alert ID:Analysis Engine内でユニークなAlertの識別子
- Engine-type: Analysis Engineの種類の識別子
- Engine-ID: 同一Mitigationに帰属する同種のAnalysis Engineの識別子
- Node-ID: Analysis Engineが帰属するMitigationのノード識別子

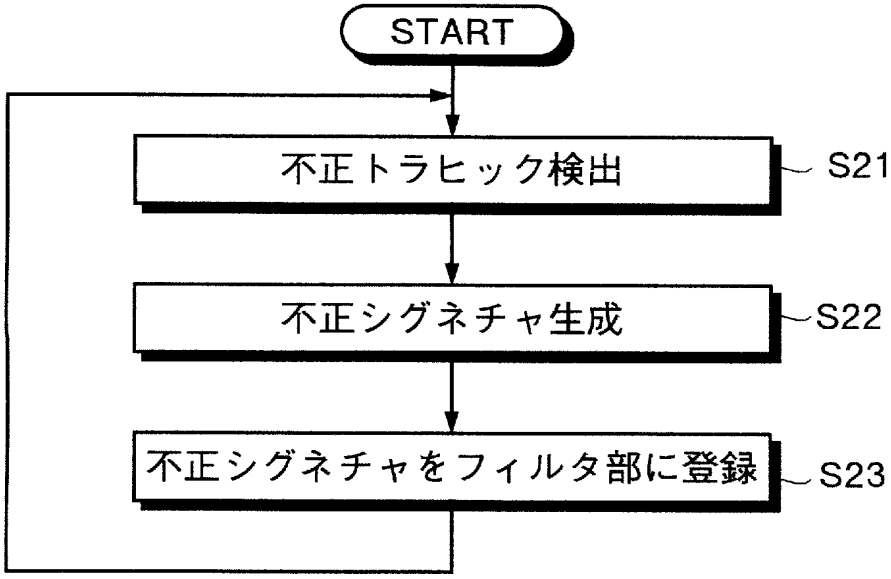
【図８】


START
攻撃容疑トラヒック検出
S1
容疑シグネチャ・
正規シグネチャ生成
S2
識別情報生成
S3
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S4
隣接関係をもつ中継装置に
容疑シグネチャ・正規条件・
識別情報を送信
S5

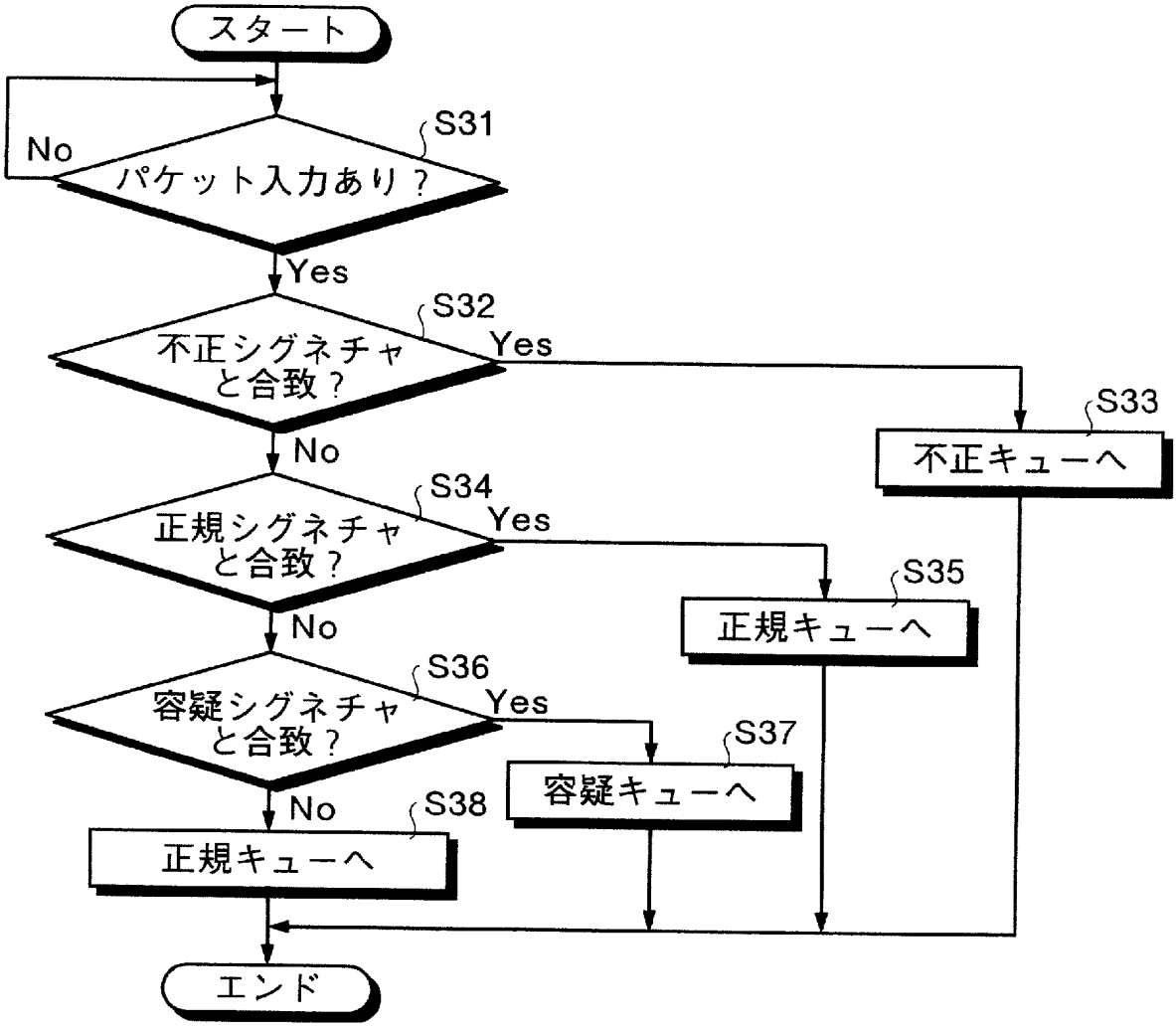
【図９】


START
S11
容疑シグネチャ・正規条件・識別情報を受信
S12
識別情報が同一？
Yes
No
S13
下流ノードが同一であるか？
No
Yes
S131
通知情報送信
S132
容疑シグネチャをフィルタ部に上書き登録
S133
正規シグネチャ生成
S134
正規シグネチャをフィルタ部に上書き登録
S135
先に送信した中継装置に容疑シグネチャ・正規条件・識別情報を再送信
S14
容疑シグネチャをフィルタ部に登録
S15
正規シグネチャ生成
S16
正規シグネチャをフィルタ部に登録
S17
隣接関係をもつ中継装置に容疑シグネチャ・正規条件・識別情報を送信

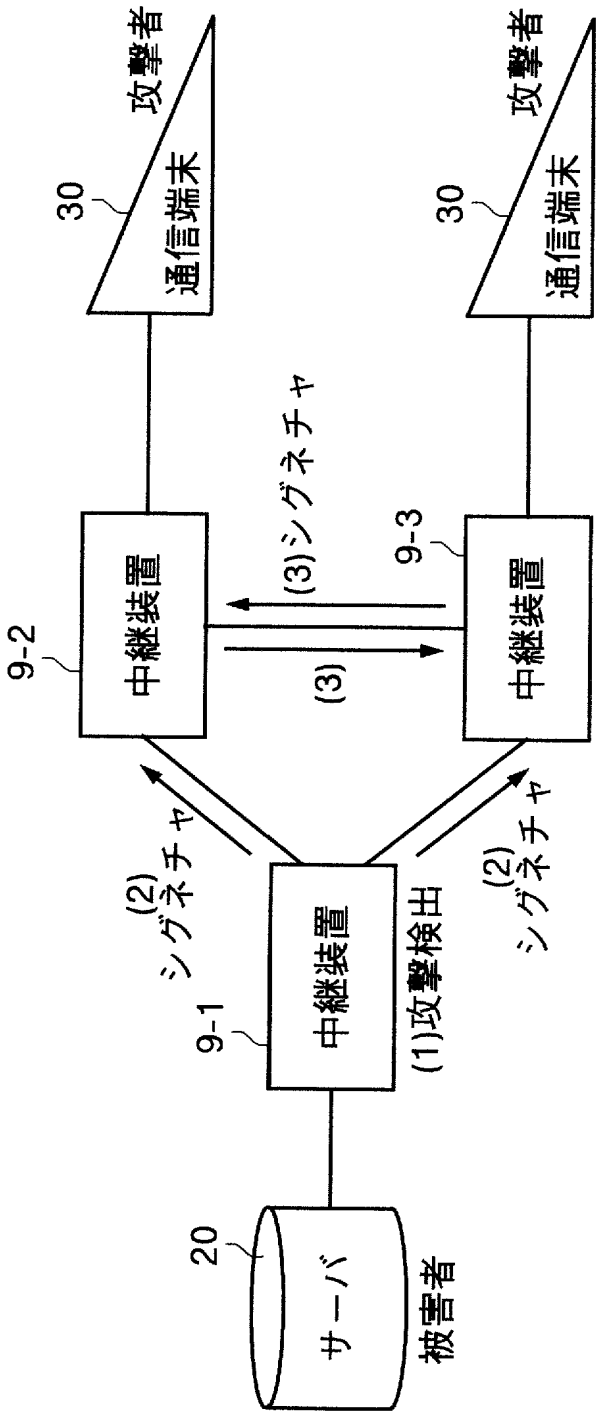
【図１０】



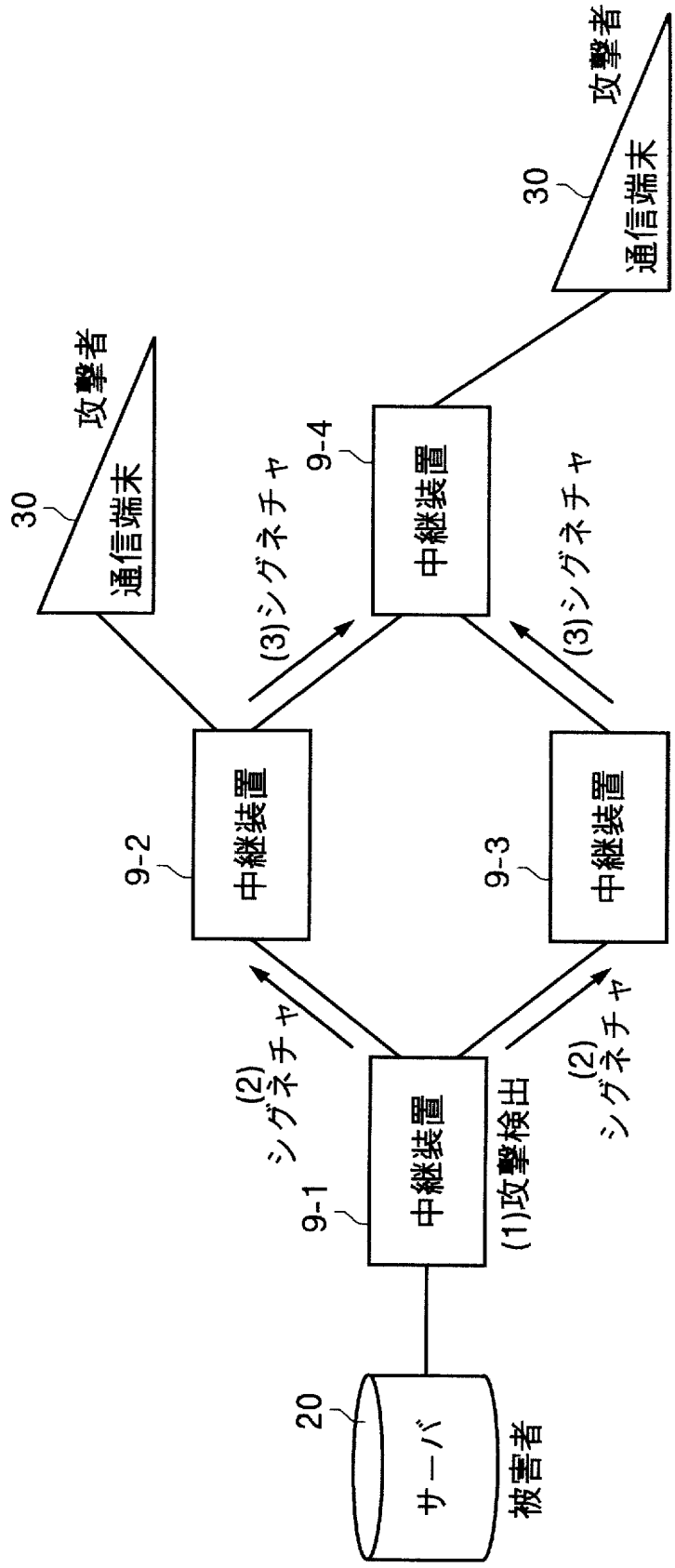
【図１１】


スタート
S31
No
パケット入力あり？
Yes
S32
不正シグネチャと合致？
Yes
S33
不正キューへ
No
S34
正規シグネチャと合致？
Yes
S35
正規キューへ
No
S36
容疑シグネチャと合致？
Yes
S37
容疑キューへ
No
S38
正規キューへ
エンド

【図１２】


攻撃者
通信端末
30
攻撃者
通信端末
30
9-2
中継装置
(3)シグネチャ
(3)
9-3
中継装置
(2)
シグネチャ
9-1
中継装置
(1)攻撃検出
(2)
シグネチャ
20
サーバ
被害者

【図１３】


攻撃者
30
通信端末
攻撃者
30
通信端末
(3)シグネチャ
9-4
中継装置
(3)シグネチャ
9-2
中継装置
9-3
中継装置
(2)
シグネチャ
9-1
中継装置
(1)攻撃検出
(2)
シグネチャ
20
サーバ
被害者

【書類名】要約書
【要約】
【課題】シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことを課題とする。
【解決手段】容疑のかかる攻撃を検出した中継装置１０では、攻撃容疑パケットを制限するための容疑シグネチャおよび容疑シグネチャの生成を一意に識別するための識別情報を生成するとともに、生成した容疑シグネチャおよび識別情報を隣接中継装置に送信する。かかる容疑シグネチャおよび識別情報を受信した中継装置１０では、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合には、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。
【選択図】　図１

出願人履歴

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社